

SOME PROPERTIES OF SKEW CODES OVER FINITE FIELDS

LUIS FELIPE TAPIA CUITIÑO AND ANDREA LUIGI TIRONI

ABSTRACT. After recalling the definition of codes as modules over skew polynomial rings, whose multiplication is defined by using an automorphism and a derivation, and some basic facts about them, in the first part of this paper we study some of their main algebraic and geometric properties. Finally, for module skew codes constructed only with an automorphism, we give some BCH type lower bounds for their minimum distance.

INTRODUCTION

In the framework of linear codes, the introduction of the cyclic codes has been important due to the fact that for the first time some special linear codes could be treated by polynomial rings via a vector space isomorphism. The use of Ore polynomial rings in the non-commutative setting emerged only recently in Coding Theory as source of generalizations of the cyclic codes. The skew polynomial rings have found applications in the construction of many algebraic codes of good parameters with respect to the commutative case. In particular, the research on codes in this setting has resulted in the discovery of many new codes with better Hamming distance than any previously known linear code with same parameters (see for instance Tables 1, 2 and 3 of [2]).

Inspired by the recent works [2] and [3], in §1 we give a background material and the notion of skew generalized cyclic (GC) codes, that is, linear codes invariant by a pseudo-linear transformation (see Definition (Δ)). In §2, we introduce some basic properties of skew GC codes and we give a result (Theorem 2.6) about duals of skew GC codes that improves Theorem 23 in [8]. Moreover, in Theorem 2.8 we show a fundamental geometric property of these codes which becomes a useful tool to find codes through the factorization of polynomials. In the commutative case ($\theta = id$), the same result delivers more geometric consequences described in Corollary 2.10. Furthermore, assumption (#) and its properties allow us to extend to the non-commutative case some of the main results of [7] (see Propositions 2.15 and 2.19). In §3 we consider the cases with trivial derivation ($\delta_\beta^\theta = 0$) by studying the minimal polynomial of a semi-linear transformation in Theorem 3.3 and some BCH lower bounds which generalize known results of [2] and [4] in the non-commutative case (see Theorems 3.9, 3.12, 3.15 and Corollary 3.17). Finally, in §4 we give some Magma programs and examples as immediate applications of some previous results.

Date: July 13, 2015.

2010 *Mathematics Subject Classification.* Primary: 12Y05, 16Z05; Secondary: 94B05, 94B35.

Key words and phrases: finite fields, dual codes, skew polynomial rings, semi-linear maps.

The second author was partially supported by Proyecto VRID N. 214.013.039-1.OIN.

1. NOTATION AND BACKGROUND MATERIAL

Denote by $\theta : \mathbb{F}_q \rightarrow \mathbb{F}_q$ an automorphism of the finite field \mathbb{F}_q . Let us recall here that if $q = p^s$ for some prime number p , then the map $\tilde{\theta} : \mathbb{F}_q \rightarrow \mathbb{F}_q$ defined by $\tilde{\theta}(a) = a^p$ is an automorphism on the field \mathbb{F}_q which fixes the subfield with p elements. This automorphism $\tilde{\theta}$ is called the *Frobenius automorphism* and it has order s . Moreover, it is known that the cyclic group it generates is the full group of automorphisms of \mathbb{F}_q , i.e. $\text{Aut}(\mathbb{F}_q) = \langle \tilde{\theta} \rangle$. Therefore, any $\theta \in \text{Aut}(\mathbb{F}_q)$ is defined as $\theta(a) := \tilde{\theta}^t(a) = a^{p^t}$, where $a \in \mathbb{F}_q$ and t is an integer such that $0 \leq t \leq s$. Furthermore, when θ will be the identity automorphism $id : \mathbb{F}_q \rightarrow \mathbb{F}_q$, we will write simply $\theta = id$. Finally, a θ -derivation must be of the form $\beta(\theta(a) - a)$ for any $a \in \mathbb{F}_q$ and some $\beta \in \mathbb{F}_q$.

A pseudo-linear map (or a pseudo-linear transformation) $T : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is an additive map defined by

$$(\Delta) \quad T(\vec{v}) := (\vec{v})\Theta \circ M + (\vec{v})\delta_\beta^\theta,$$

where $(v_1, \dots, v_n)\Theta := (\theta(v_1), \dots, \theta(v_n))$, M is an $n \times n$ matrix with coordinates in \mathbb{F}_q and $(v_1, \dots, v_n)\delta_\beta^\theta := (\beta(\theta(v_1) - v_1), \dots, \beta(\theta(v_n) - v_n))$. When $\delta_\beta^\theta = 0$, we call T a *semi-linear map*, or a *semi-linear transformation*.

Consider the ring structure defined on the following set:

$$R := \mathbb{F}_q[X; \theta, \delta_\beta^\theta] = \{a_s X^s + \dots + a_1 X + a_0 \mid a_i \in \mathbb{F}_q \text{ and } s \in \mathbb{N}\}.$$

The addition in R is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X \cdot a = \theta(a)X + \beta(\theta(a) - a)$ for any $a \in \mathbb{F}_q$ and extended to all elements of R by associativity and distributivity. The ring R is known as skew polynomial ring and its elements are skew polynomials. Moreover, it is a left and right Euclidean ring whose left and right ideals are principals.

From now on, fix a polynomial

$$(*) \quad f := X^n - f_{n-1}X^{n-1} - \dots - f_1X - f_0 \in R$$

and denote by $\pi_f : \mathbb{F}_q^n \rightarrow R/Rf$ the linear transformations which sends a vector $(c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n$ to the polynomial class $\left[\sum_{i=0}^{n-1} c_i X^i\right] \in R/Rf$, i.e.

$$\pi_f((c_0, \dots, c_{n-1})) := \left[\sum_{i=0}^{n-1} c_i X^i\right] \in R/Rf \quad \forall (c_0, \dots, c_{n-1}) \in \mathbb{F}_q^n.$$

With an abuse of notation, a polynomial $c \in R$ and its class $[c] \in R/Rf$ will be denoted sometimes with the same letter c for simplicity.

Let us introduce here a generalization of the skew cyclic codes.

Definition 1.1. A linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is called a $(M, \Theta, \delta_\beta^\theta)$ -**code** if $T \star \mathcal{C} \subseteq \mathcal{C}$, where T is as in (Δ) and $T \star \mathcal{C} := \{T(\vec{v}) \mid \vec{v} \in \mathcal{C}\}$. Moreover, $\mathcal{C} \subseteq \mathbb{F}_q^n$ is called a $(f, \Theta, \delta_\beta^\theta)$ -**skew generalized cyclic (GC) code** (or, for simplicity, a **skew GC code**) if $T_f \star \mathcal{C} \subseteq \mathcal{C}$, where T_f is the pseudo-linear map defined by $T_f(\vec{v}) := (\vec{v})\Theta \circ A + (\vec{v})\delta_\beta^\theta$ with

$$(**) \quad A := \left(\begin{array}{c|cccc} 0 & 1 & & & \\ \vdots & & \ddots & & \\ 0 & & & 1 & \\ \hline f_0 & f_1 & \cdots & f_{n-1} & \end{array} \right).$$

Finally, when $\theta = \text{id}$, a $(f, \Theta, \delta_\beta^\theta)$ -skew generalized cyclic (GC) code is called an ***f-generalized cyclic (GC) code***, or simply a ***GC code***.

Remark 1.2. Suppose that $\theta = \text{id}$ and $f = X^n - f_{n-1}X^{n-1} \dots - f_1X - f_0$ is the minimal polynomial of an $n \times n$ matrix M . Then by [5, Lemma 6.7.1] there is a basis $\{\vec{r}_1, \dots, \vec{r}_n\}$ of \mathbb{F}_q^n such that

$$M = S \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \cdots & f_{n-1} \end{array} \right) S^{-1}$$

where $S = (\vec{r}_{1t} \mid \cdots \mid \vec{r}_{nt})$. Therefore the $n \times n$ matrix M is similar to its rational canonical form A , i.e. there exists a non-singular matrix S such that

$$(\circ) \quad M = SAS^{-1}.$$

Let $\mathcal{C}_M \subseteq \mathbb{F}_q^n$ be a linear code invariant by the matrix M . Define

$$\mathcal{C}_A := \mathcal{C}_M \star S := \{\vec{c}S : \vec{c} \in \mathcal{C}_M\}.$$

Then by (\circ) we obtain

$$\mathcal{C}_A \star A = \mathcal{C}_M \star (SA) = \mathcal{C}_M \star (S(S^{-1}MS)) = (\mathcal{C}_M \star M) \star S \subseteq \mathcal{C}_M \star S = \mathcal{C}_A,$$

i.e. \mathcal{C}_A is invariant by A . Since S is an invertible matrix, this shows that we can construct a one-to-one correspondence between the set of linear codes invariant by A and the set of linear codes invariant by M .

2. BASIC PROPERTIES OF SKEW GC CODES

In this section, we give some algebraic and geometric properties of skew generalized cyclic (GC) codes.

Remark 2.1. Let T be any pseudo-linear transformation on \mathbb{F}_q^n . If $p = p_0 + p_1X + \dots + p_mX^m$ is a polynomial, then $p(T) = p_0 + p_1T + \dots + p_mT^m$ is not in general a pseudo-linear transformation. On the other hand, a linear subspace $U \subseteq \mathbb{F}_q^n$ is T -invariant, i.e. $T \star U \subseteq U$, if and only if $p(T) \star U \subseteq U$ for any polynomial p .

Remark 2.2. We have $p(X) \cdot \pi_f(\vec{v}) = \pi_f(p(T_f)(\vec{v}))$ for any polynomial p and all $\vec{v} \in \mathbb{F}_q^n$.

From Remarks 2.1 and 2.2, we deduce the following characterization of a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code.

Proposition 2.3. Let \mathcal{C} be a non-empty subset of \mathbb{F}_q^n . Then

$$\mathcal{C} \text{ is a } (f, \Theta, \delta_\beta^\theta)\text{-skew GC code} \iff \pi_f(\mathcal{C}) \text{ is a principal left ideal of } R/Rf.$$

Remark 2.4. By Proposition 2.3, we see that to produce examples of $(f, \Theta, \delta_\beta^\theta)$ -skew GC codes one can focus on finding right divisors of f .

Definition 2.5. For any $(f, \Theta, \delta_\beta^\theta)$ -skew GC code $\mathcal{C} \subseteq \mathbb{F}_q^n$, the generator polynomial of $\pi_f(\mathcal{C}) \subseteq R/Rf$ is called the **generator polynomial** of \mathcal{C} .

Therefore, we will write $\mathcal{C} = (g)_{n,q}^{\theta, \delta_\beta^\theta}$ for a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with generator polynomial $g = g_0 + g_1X + \dots + g_{n-k}X^{n-k} \in R/Rf$.

From [2] we know that a generator matrix of a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code $\mathcal{C} = (g)_{n,q}^{\theta, \delta_\beta^\theta}$ is given by

$$G := \begin{pmatrix} \vec{g} \\ T_f(\vec{g}) \\ \vdots \\ T_f^{k-1}(\vec{g}) \end{pmatrix},$$

where $\vec{g} = \pi_f^{-1}(g)$.

About the dual code \mathcal{C}^\perp of a $(M, \Theta, \delta_\beta^\theta)$ -code $\mathcal{C} \subseteq \mathbb{F}_q^n$, we can give the following

Theorem 2.6. *If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is a $(M, \Theta, \delta_\beta^\theta)$ -code, then \mathcal{C}^\perp is a $((M_t)_{\theta^{-1}}, \Theta^{-1}, \delta_{\theta^{-1}(\beta)}^{\theta^{-1}})$ -code, where $W_{\theta^{-1}} := [\theta^{-1}(a_{ij})]$ and W_t is the transpose matrix of a matrix $W = [a_{ij}]$.*

Proof. Denote by T' the pseudo-linear map defined by $T'(\vec{v}) := (\vec{v})\Theta^{-1} \circ (M_t)_{\theta^{-1}} + (\vec{v})\delta_{\theta^{-1}(\beta)}^{\theta^{-1}}$. For any $\vec{c} \in \mathcal{C}$ and $\vec{a} \in \mathcal{C}^\perp$, note that

$$\begin{aligned} 0 &= \vec{a} \cdot T_f(\vec{c}) = \vec{a} \cdot ((\vec{c})\Theta \circ M) + \vec{a} \cdot ((\vec{c})\delta_\beta^\theta) = \\ &= (\vec{a}M_t) \cdot ((\vec{c})\Theta) + \vec{a} \cdot ((\vec{c})\Theta\beta) = (\vec{a}M_t + \beta\vec{a}) \cdot ((\vec{c})\Theta), \end{aligned}$$

i.e. $(\vec{a}M_t + \beta\vec{a}) \cdot ((\vec{c})\Theta) = 0$. Thus by [8, Lemma 4] we conclude that

$$\begin{aligned} (T'(\vec{a})) \cdot \vec{c} &= ((\vec{a})\Theta^{-1} \circ (M_t)_{\theta^{-1}} + (\vec{a})\delta_{\theta^{-1}(\beta)}^{\theta^{-1}}) \cdot \vec{c} = \\ &= ((\vec{a})\Theta^{-1} \circ (M_t)_{\theta^{-1}} + ((\vec{a})\Theta^{-1} - \vec{a})\theta^{-1}(\beta)) \cdot \vec{c} \\ &= ((\vec{a})(M_t) \circ \Theta^{-1} + (\beta\vec{a})\Theta^{-1}) \cdot \vec{c} = ((\vec{a})(M_t) + (\beta\vec{a}))\Theta^{-1} \cdot \vec{c} = 0. \end{aligned}$$

for every $\vec{a} \in \mathcal{C}^\perp$ and $\vec{c} \in \mathcal{C}$. \square

Definition 2.7. *A polynomial $p \in R$ is invariant if $Rp = pR$. Moreover, the set of all invariant polynomials in R will be denoted by $N(R)$.*

Let us prove now the following

Theorem 2.8. *Let $f \in R$ be as in (*) and let T_f be its associated pseudo-linear transformation as in (**). Then the following properties hold:*

- (1) *If $f = h \cdot g$ for some $h, g \in R$, then*

$$Rg/Rf = \pi_f(\text{Ker } h(T_f)) \iff h \in N(R);$$

- (2) *If $f = h \cdot g = g \cdot h'$ for some $h, h', g \in R$, e.g. when $g \in N(R)$, then $\deg g$ linearly independent columns of the $n \times n$ matrix*

$$\begin{pmatrix} \pi_f^{-1}(h') \\ T_f(\pi_f^{-1}(h')) \\ \vdots \\ T_f^{n-1}(\pi_f^{-1}(h')) \end{pmatrix}$$

form a basis of \mathcal{C}^\perp , where $\mathcal{C} = (g)_{n,q}^{\theta, \delta_\beta^\theta}$.

Proof. (1) Assume that $h \in N(R)$. If $a \in Rg/Rf$ then $a = \alpha g$ and

$$h\alpha g = \alpha' hg = \alpha' f = 0 \in R/Rf.$$

Then we have

$$\vec{0} = \pi_f^{-1}(h\alpha g) = h(T_f)\pi_f^{-1}(\alpha g).$$

This shows that $a = \alpha g \in \pi_f(\text{Ker } h(T_f))$, that is, $Rg/Rf \subseteq \pi_f(\text{Ker } h(T_f))$.

On the other hand, if $v \in \pi_f(\text{Ker } h(T_f))$ then $h(T_f)\pi_f^{-1}(v) = \vec{0}$. Hence $hv = \beta f$ for some $\beta \in R$ and this gives

$$hv = \beta f = \beta hg = h\beta' g,$$

i.e. $v = \beta' g \in Rg/Rf$. Thus $\pi_f(\text{Ker } h(T_f)) \subseteq Rg/Rf$, i.e. $Rg/Rf = \pi_f(\text{Ker } h(T_f))$.

Conversely, suppose that $Rg/Rf = \pi_f(\text{Ker } h(T_f))$. Let $\alpha \in R$ and write $\alpha g = \pi_f(\vec{v})$, where $\vec{v} \in \text{Ker } h(T_f)$. Then

$$h\alpha g = h\pi_f(\vec{v}) = \pi_f(h(T_f)\vec{v}) = \pi_f(\vec{0}) = 0 \in R/Rf.$$

This shows that there exists an element $q \in R$ such that $h\alpha g = qf = qhg$, i.e. $h\alpha = qh$. Hence $h \in N(R)$.

(2) Let $\vec{c} \in \mathcal{C}$ and write $\pi_f(h'\vec{c}) = h'$ and $\pi_f(\vec{c}) = c = \alpha g$, for some $\alpha, c \in R$. Then we get

$$\pi_f(c(T_f)(h'\vec{c})) = ch' = (\alpha g)h' = \alpha(gh') = \alpha f = 0 \in R/Rf,$$

i.e. $c(T_f)(h'\vec{c}) = \vec{0}$. Write $\vec{c} = (c_0, \dots, c_{n-1})$. Therefore we have

$$\vec{0} = c(T_f)(h'\vec{c}) = c_0 h'\vec{c} + c_1 T_f(h'\vec{c}) + \dots + c_{n-1} T_f^{n-1}(h'\vec{c}).$$

This shows that

$$(c_0, \dots, c_{n-1}) \cdot \begin{pmatrix} h'\vec{c} \\ T_f(h'\vec{c}) \\ \vdots \\ T_f^{n-1}(h'\vec{c}) \end{pmatrix} = \vec{0}$$

for any $\vec{c} = (c_0, \dots, c_{n-1}) \in \mathcal{C}$. Finally, since $\pi_f(T_f^k(h'\vec{c})) = X^k h'$ for $k = 0, \dots, n - \deg h' - 1 = \deg g - 1$, we see that $\{h'\vec{c}, T_f(h'\vec{c}), \dots, T_f^{\deg g - 1}(h'\vec{c})\}$ are linearly independent. \square

From the above result, we can deduce the following consequences.

Corollary 2.9. *Suppose that the same hypothesis as in Theorem 2.8(1) holds. Then*

$$\text{Ker } h(T_f) \subseteq \mathbb{F}_q^n \text{ is a } (f, \Theta, \delta_\beta^\theta)\text{-skew GC code} \iff h \in N(R).$$

Corollary 2.10. *Assume that $\theta = \text{id}$ and let $f \in \mathbb{F}_q[X]$. Then we have the following properties:*

- (1) *If $f = h \cdot g$ for some $h, g \in \mathbb{F}_q[X]$, then $(g) = \pi_f(\text{ker } h(A))$;*
- (2) *$\text{ker } h'(A) \subseteq \mathbb{F}_q^n$ is a vector subspace invariant by A for any divisor h' of f ;*
- (3) *all the f -GC codes are given by $\text{ker } h''(A)$, where h'' is a divisor of f ;*
- (4) *If \mathcal{C} is an f -GC code such that $\pi_f(\mathcal{C}) = (g)$, then $n - \dim \mathcal{C}$ linearly independent columns of $h(A)$ form a basis of \mathcal{C}^\perp , where $f = h \cdot g$; moreover, if $b \in \mathbb{F}_q[X]$ is the smallest degree polynomial such that $\mathcal{C} \subseteq \text{ker } b(A)$, then $b = ah$ for some $a \in \mathbb{F}_q \setminus \{0\} =: \mathbb{F}_q^*$.*

Proof. Note that by Theorem 2.8(1) and Corollary 2.9 we get cases (1),(3) and (2) respectively. Let \mathcal{C} be an f -GC code such that $\pi_f(\mathcal{C}) = (g)$. Then from (1) it follows that $\mathcal{C} = \ker h(A)$, where $f = h \cdot g$. Since $\text{rk} h(A) = n - \dim \ker h(A) = n - \dim \mathcal{C}$, we deduce that $n - \dim \mathcal{C}$ linearly independent columns of $h(A)$ form a basis of \mathcal{C}^\perp . Finally, assume that $\mathcal{C} \subseteq \ker b(A)$ for some $b \in \mathbb{F}_q[X]$ with smallest degree. Then $h = bq + r$ for some $q, r \in \mathbb{F}_q[X]$ such that $\deg r < \deg b$. Since $h(A) = b(A)q(A) + r(A)$, we see that $\mathcal{C} \subseteq \ker r(A)$. Thus $r = 0$ and $h = bq$. Hence $f = b \cdot q \cdot g$ and this gives $(g) = \pi_f(\mathcal{C}) \subseteq \pi_f(\ker b(A)) = (qg)$. Therefore, we have $g = \alpha qg + \beta f$ for some $\alpha, \beta \in \mathbb{F}_q[X]$, i.e. $1 = (\alpha q + \beta b)q$. This shows that $q \in \mathbb{F}_q^*$ and that $b = ah$ with $a = q^{-1}$. \square

The next useful result is related to polynomials in $N(R)$.

Lemma 2.11. *Let $a, b \in N(R)$ such that $a = bc = c'b$ for some $c, c' \in R$. Then $c, c' \in N(R)$.*

Proof. Assume that $a = bc$ for some $c \in R$. Then for any $d \in R$ we have

$$b(cd) = (bc)d = ad = d'a = d'(bc) = (d'b)c = (bd'')c = b(d''c),$$

for some $d', d'' \in R$, i.e. $cd = d''c$. Similarly, one can prove that for any $e \in R$ there exists $e' \in R$ such that $c'e = e'c'$. This shows that $c, c' \in N(R)$. \square

From now on, assume that

(#) $f = f_1^{\alpha_1} \cdots f_t^{\alpha_t}$ is a factorization of f as in (*) into monic polynomials $f_k \in N(R)$ which are irreducible in $N(R)$ and such that $Rf_i \neq Rf_j$ for any $i \neq j$.

Remark 2.12. *If $\theta = id$, then we have $\delta_\beta^\theta = 0$ and (#) always holds.*

On the other hand, when either $\theta \neq id$ or $\delta_\beta^\theta \neq 0$, we have the following

Proposition 2.13. *(#) holds $\iff f \in N(R)$.*

Proof. If (#) holds, then $f \in N(R)$ because the product of elements in $N(R)$ belongs in $N(R)$. Assume now that $f \in N(R)$. By [6, Theorem 9, p.38] we know that $Rf = Rf_1^{\beta_1} \cdots Rf_s^{\beta_s}$ with $\beta_j \in \mathbb{Z}_{\geq 0}$, f_j a monic polynomial in $N(R)$ and Rf_j a maximal two sided ideal for any $j = 1, \dots, s$. This shows that $f_i \neq f_j$ and that all the f_i 's are irreducible polynomials in $N(R)$. Thus $f = hf_1^{\beta_1} \cdots f_s^{\beta_s}$ for some $h \in R$. Since f and all the f_j 's are polynomials in $N(R)$, from Lemma 2.11 it follows that $h \in N(R)$. Then $f = f'h$ for some $f' \in R$ and this gives that $Rf = R(f'h) \subseteq Rh$. Hence Rh is a two sided ideal containing Rf and from [6, p.38] we deduce that $Rh = Rf_1^{\gamma_1} \cdots Rf_s^{\gamma_s}$, where $\gamma_i \in \mathbb{Z}_{\geq 0}$ and $\gamma_i \leq \beta_i$ for every $i = 1, \dots, s$. Therefore we get that

$$Rf_1^{\beta_1} \cdots Rf_s^{\beta_s} = Rf = R(h) \cdot R(f_1^{\beta_1}) \cdots R(f_s^{\beta_s}) = R(f_1)^{\beta_1 + \gamma_1} \cdots R(f_s)^{\beta_s + \gamma_s},$$

and since the factorization of Rf is unique, we conclude that $\gamma_i = 0$ for any $i = 1, \dots, s$, i.e. $Rh = R$. Hence $h \in \mathbb{F}_q^\theta$ and since f is a monic polynomial, we obtain that $h = 1$. \square

Lemma 2.14. *Assume that (#) holds. Then for any $a_m, b_m \in \mathbb{Z}_{>0}$ we have the following two properties:*

- (a) $\text{lgcd}(\prod_{k=1}^r f_{i_k}^{a_k}, \prod_{h=1}^s f_{j_h}^{b_h}) = 1$, for any $\{j_1, \dots, j_s\} \subseteq \{1, \dots, t\} \setminus \{i_1, \dots, i_r\}$;
- (b) $f_i^{a_i} f_j^{b_j} = f_j^{b_j} f_i^{a_i}$.

Proof. (a) For simplicity of notation write $g_i := \prod_{k=1}^r f_{i_k}^{a_k}$, $g_j := \prod_{h=1}^s f_{j_h}^{b_h}$ and $\text{lgcd}(g_i, g_j) = d_{ij}$, where d_{ij} is a monic polynomial in R . Note that in fact $d_{ij} \in N(R)$. Since $Rg_i + Rg_j = Rd_{ij}$, we deduce that there exist $a, b \in N(R)$ such that $g_i = ad_{ij}$ and $g_j = bd_{ij}$. Thus $Rg_i \subseteq Rd_{ij}$ and $Rg_j \subseteq Rd_{ij}$. By [6, p.38] we deduce that

$$Rd_{ij} = \prod_{k=1}^r (Rf_{i_k})^{c_k} = \prod_{h=1}^s (Rf_{j_h})^{d_h},$$

where $0 \leq c_k \leq a_k$ and $0 \leq d_h \leq b_h$. From the uniqueness of the decomposition, we deduce that $c_k = 0$ and $d_h = 0$ for $k = 1, \dots, r$ and $h = 1, \dots, s$. Hence $Rd_{ij} = R$, that is, $d_{ij} = 1$.

(b) Observe that the statement follows from $f_i f_j = f_j f_i$. So, assume that $a_i = b_j = 1$. From [6, Lemma 4, p.38] we deduce that $Rf_i \cdot Rf_j = Rf_j \cdot Rf_i$. This shows that there exist $u, v \in R$ such that $f_i f_j = u f_j f_i$ and $v f_i f_j = f_j f_i$. Therefore we get $f_i f_j = u f_j f_i = uv f_i f_j$, i.e. $uv = 1$. So $u \in \mathbb{F}_q^*$ and $f_i f_j = u f_j f_i$. Since all the f_k 's are monic polynomials, we see that $u = 1$. \square

In line with [7], consider now the following subsets of \mathbb{F}_q^n

$$(1) \quad U_i := \text{Ker } f_i^{\alpha_i}(T_f)$$

for $i = 1, \dots, t$, where T_f is as in (**). Then we have the following properties for the U_i 's.

Proposition 2.15. *Under assumption (#), for the linear subspaces U_i of \mathbb{F}_q^n we get the following properties:*

- (a) U_i is a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code;
- (b) $\dim U_i = \alpha_i \deg(f_i)$ for $i = 1, \dots, t$;
- (c) $\mathbb{F}_q^n = U_1 \oplus \dots \oplus U_t$;
- (d) if \mathcal{C} is a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code and $\mathcal{C}_i := \mathcal{C} \cap U_i$ for $i = 1, \dots, t$, then \mathcal{C}_i is a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code and $\mathcal{C} = \mathcal{C}_1 \oplus \dots \oplus \mathcal{C}_t$;
- (e) If $\alpha_i = 1$ and f_i is irreducible in R for some $i \in \{1, \dots, t\}$, then U_i is minimal with respect to the inclusion.

Proof. (a) Since $f_i^{\alpha_i} \in N(R)$, from Corollary 2.9 we know that $\text{Ker } f_i^{\alpha_i}(T_f)$ is a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code.

(b) By Theorem 2.8(1) and Lemma 2.14 we have $R\left(\frac{f}{f_i^{\alpha_i}}\right) = \pi_f(\text{Ker } f_i^{\alpha_i}(T_f))$. Thus we deduce that

$$\dim U_i = \dim \text{Ker } f_i^{\alpha_i}(T_f) = \deg f - \deg \left(\frac{f}{f_i^{\alpha_i}} \right) = \deg f_i^{\alpha_i} = \alpha_i \deg f_i.$$

(c) Since R is a principal ideal domain and the sum of two sided ideal is a two sided ideal, write $Rm = R\hat{f}_1 + \dots + R\hat{f}_t$ for some $m \in N(R)$, where $\hat{f}_i := \frac{f}{f_i^{\alpha_i}}$ for every $i = 1, \dots, t$. Moreover, by Lemma 2.11 note that $\hat{f}_i = a_i m$ for some $a_i \in N(R)$ and every $i = 1, \dots, t$. Since

$$(Rf_1)^{\alpha_1} \cdot \dots \cdot (Rf_{i-1})^{\alpha_{i-1}} \cdot (Rf_{i+1})^{\alpha_{i+1}} \cdot \dots \cdot (Rf_t)^{\alpha_t} = R\hat{f}_i \subset Rm,$$

from [6, p. 38] it follows that

$$Rm = (Rf_1)^{\beta_1} \cdot \dots \cdot (Rf_{i-1})^{\beta_{i-1}} \cdot (Rf_{i+1})^{\beta_{i+1}} \cdot \dots \cdot (Rf_t)^{\beta_t},$$

where $0 \leq \beta_k \leq \alpha_k$ for $k = 1, \dots, i-1, i+1, \dots, t$. So we have

$Rm = (Rf_2)^{\beta_2} \dots (Rf_t)^{\beta_t} = (Rf_1)^{\beta_1} (Rf_3)^{\beta_3} \dots (Rf_t)^{\beta_t} = \dots = (Rf_1)^{\beta_1} \dots (Rf_{t-1})^{\beta_{t-1}}$,
and by Theorem 9 of [6, p. 38] we deduce that $Rm = R$, i.e. $R = R\hat{f}_1 + \dots + R\hat{f}_t$.
Thus $1 = a_1\hat{f}_1 + \dots + a_t\hat{f}_t$ for some $a_1, \dots, a_t \in R$. This gives $X^h = (X^h a_1)\hat{f}_1 + \dots + (X^h a_t)\hat{f}_t$ for every $h = 0, \dots, n-1$. Therefore, for any $\vec{v} = (v_0, \dots, v_{n-1}) \in \mathbb{F}_q^n$, we get

$$\begin{aligned} \vec{v} &= \sum_{i=0}^{n-1} v_i \pi_f^{-1}(X^i) = \sum_{i=0}^{n-1} v_i \pi_f^{-1} \left(\sum_{j=1}^t (X^i a_j) \hat{f}_j \right) = \\ &= \sum_{j=1}^t \pi_f^{-1} \left[\left(\sum_{i=0}^{n-1} v_i X^i \right) a_j \hat{f}_j \right] \in \pi_f^{-1} (R\hat{f}_1) + \dots + \pi_f^{-1} (R\hat{f}_t), \end{aligned}$$

i.e. $\vec{v} \in U_1 + \dots + U_t$ by Theorem 2.8(1). Hence $\mathbb{F}_q^n = U_1 + \dots + U_t$.

Finally, observe that $R\hat{f}_i \cap R\hat{f}_j = RM_{ij}$ with $M_{ij} \in N(R)$ for any $i \neq j$. Moreover, $M_{ij} = a_i \hat{f}_i = a_j \hat{f}_j$ for some $a_i, a_j \in N(R)$. This gives $a_i f_j^{\alpha_j} = a_j f_i^{\alpha_i}$ and then $Ra_i \cdot (Rf_j)^{\alpha_j} = Ra_j \cdot (Rf_i)^{\alpha_i}$. From [6, Theorem 9, p.38] it follows that $Ra_i = Rh \cdot (Rf_i)^{\alpha_i}$ for some $h \in R$, i.e. $a_i = a f_i^{\alpha_i}$ for some $a \in N(R)$ by Lemma 2.11. Therefore, $M_{ij} = af$ and we conclude that

$$U_i \cap U_j = \pi_f^{-1}(R\hat{f}_i \cap R\hat{f}_j) = \pi_f^{-1}(R(af)) \subseteq \pi_f^{-1}(Rf) = \vec{0}$$

for any $i \neq j$, that is, $\mathbb{F}_q^n = U_1 \oplus \dots \oplus U_t$.

(d) From (a), it follows that each $\mathcal{C}_i := \mathcal{C} \cap U_i$ is a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code of \mathbb{F}_q^n . Furthermore, from (c) we can deduce that

$$\mathcal{C} = \mathcal{C} \cap \mathbb{F}_q^n = \mathcal{C} \cap (U_1 \oplus \dots \oplus U_t) = (\mathcal{C} \cap U_1) \oplus \dots \oplus (\mathcal{C} \cap U_t) = \mathcal{C}_1 \oplus \dots \oplus \mathcal{C}_t.$$

(e) For simplicity, assume that $i = 1$. Let U be a $(f, \Theta, \delta_\beta^\theta)$ -skew GC code such that

$$\{\vec{0}\} \subseteq U \subseteq U_1 := \text{Ker} f_1(A).$$

Then by Proposition 2.3 and Theorem 2.8(1) we know that there exists a right divisor $g' \in R$ of f such that $f = h'g'$ and $Rg' = \pi_f(U) \subseteq \pi_f(U_1) = R\frac{f}{f_1}$. Hence there is a polynomial $q \in R$ such that $g' = q \cdot f_2^{\alpha_1} \cdot \dots \cdot f_t^{\alpha_t}$ and this gives

$$f_1 \cdot f_2^{\alpha_2} \cdot \dots \cdot f_t^{\alpha_t} = f = h'g' = (h'q) \cdot f_2^{\alpha_1} \cdot \dots \cdot f_t^{\alpha_t},$$

i.e. $f_1 = h'q$. Since f_1 is irreducible in R , we conclude that either $\deg q = 0$ or $q = f_1$. Therefore, we have either $U = \pi_f^{-1}(Rg') = \pi_f^{-1}(R\frac{f}{f_1}) = U_1$ or $U = \pi_f^{-1}(Rg') = \pi_f^{-1}(Rf) = \{\vec{0}\}$. \square

Proposition 2.16. *Let $f \in R$. Then $f \in N(R) \iff f(T_f) = 0$.*

Proof. Assume that $f \in N(R)$. Then for every $\vec{v} = \pi_f^{-1}(v) \in \mathbb{F}_q^n$, from Remark 2.2 we conclude that

$$\pi_f(f(T_f)\vec{v}) = f\pi_f(\vec{v}) = fv = v'f = 0 \in R/Rf,$$

for some $v' \in R$, i.e. $f(T_f)(\vec{v}) = \vec{0}$. Finally, suppose that $f(T_f) = 0$. Consider $g \in R$. If $\deg g < \deg f$, then

$$f \cdot g = f \cdot \pi_f(\pi_f^{-1}(g)) = \pi_f(f(T_f)\pi_f^{-1}(g)) = 0 \in R/Rf,$$

i.e. there exists $k \in R$ such that $f \cdot g = k \cdot f$. On the other hand, if $\deg f \leq \deg g$ then there are $q, r \in R$ such that $g = qf + r$ with $\deg r < \deg f$. Thus by the above argument, we can conclude that $f \cdot g = f \cdot (qf + r) = fqf + fr = fqf + r'f = (fq + r')f$ for some $r' \in R$. This shows that $f \in N(R)$. \square

Remark 2.17. When $\delta_\beta = 0$, then $f(T_f) = 0$ if and only if $f \in \mathbb{F}_q^\theta[X^k; \theta, 0]$ with k the orden of θ . If $\delta_\beta \neq 0$, then Proposition 2.16 gives a criterion to know when $f \in N(R)$.

Having in mind Proposition 2.13, we have the following

Corollary 2.18. $(\#)$ holds $\iff f(T_f) = 0$.

Let f be as in $(\#)$ and write $f = f_i^{\alpha_i} \cdot \widehat{f}_i$. By Lemma 2.14 we know that $\text{lgcd}(f_i^{\alpha_i}, \widehat{f}_i) = 1$. Thus there exist $a_i, b_i \in R$ such that $a_i f_i^{\alpha_i} + b_i \widehat{f}_i = 1$. So we get $(b_i \widehat{f}_i)(a_i f_i^{\alpha_i}) + (b_i \widehat{f}_i)^2 = b_i \widehat{f}_i$, i.e. $(b_i \widehat{f}_i)^2 + c_i f = b_i \widehat{f}_i$, for some $c_i \in R$. Therefore by Lemma 2.7 of [3] and Corollary 2.18 we deduce that

$$b_i(T_f) \widehat{f}_i(T_f) = (b_i(T_f) \widehat{f}_i(T_f))^2 + c_i(T_f) f(T_f) = (b_i(T_f) \widehat{f}_i(T_f))^2.$$

As in [7], define $e_i(T_f) := b_i(T_f) \widehat{f}_i(T_f)$. In the same spirit of [7] and for the convenience of the reader, we give and prove the following result.

Proposition 2.19. Under assumption $(\#)$, we get the following properties:

- (a) $e_i(T_f)^2 = e_i(T_f)$;
- (b) $e_i(T_f) e_j(T_f) = 0$ for $i \neq j$;
- (c) $e_i(T_f)(\vec{v}_j) = 0$ for every $\vec{v}_j \in U_j$ with $j \neq i$;
- (d) $\vec{v} \in U_i \iff e_i(T_f)(\vec{v}) = \vec{v}$; moreover, if T is an idempotent endomorphism of \mathbb{F}_q^n such that $\vec{v} \in U_i \iff T(\vec{v}) = \vec{v}$, then $T = e_i(T_f)$;
- (e) $\sum_{i=1}^t e_i(T_f) = id$;
- (f) If $\theta = id$, then $U_i = \langle e_i(A)_1, \dots, e_i(A)_n \rangle$, where $e_i(A)_j$ is the j^{th} row of $e_i(A)$.

Proof. (a) It follows from the definition of $e_i(T_f)$.

(b) By [3, Lemma 2.7] we deduce that

$$e_i(T_f) e_j(T_f) = (e_i e_j)(T_f) = (b_i \widehat{f}_i b_j \widehat{f}_j)(T_f) = (cf)(T_f) = c(T_f) f(T_f) = 0,$$

for some $c \in R$.

(c) Let $\vec{u}_j \in U_j$. Then there is a $t \in R$ such that

$$e_i(T_f)(\vec{u}_j) = (b_i \widehat{f}_i)(T_f)(\vec{u}_j) = (t f_j^{\alpha_j})(T_f)(\vec{u}_j) = t(T_f) f_j^{\alpha_j}(T_f)(\vec{u}_j) = 0.$$

(d) Let $\vec{v} \in U_i$. Note that

$$a_i(T_f) f_i^{\alpha_i}(T_f) + e_i(T_f) = a_i(T_f) f_i^{\alpha_i}(T_f) + b_i(T_f) \widehat{f}_i(T_f) = id.$$

Hence $e_i(T_f)(\vec{v}) = a_i(T_f) f_i^{\alpha_i}(T_f)(\vec{v}) + e_i(T_f)(\vec{v}) = \vec{v}$. On the other hand, if $e_i(T_f)(\vec{v}) = \vec{v}$ then there exists a $c \in R$ such that

$$f_i^{\alpha_i}(T_f)(\vec{v}) = (f_i^{\alpha_i} e_i)(T_f)(\vec{v}) = (f_i^{\alpha_i} b_i \widehat{f}_i)(T_f)(\vec{v}) = (cf)(T_f)(\vec{v}) = c(T_f) f(T_f)(\vec{v}) = 0,$$

i.e. $\vec{v} \in U_i$.

Let T be an idempotent endomorphism, that is $T^2 = T$, such that $\vec{v} \in U_i \iff T(\vec{v}) = \vec{v}$. Then $\text{Im}(T) = U_i$ and for every $\vec{v} \in \mathbb{F}_q^n$ we can write $\vec{v} = [\vec{v} - T(\vec{v})] + T(\vec{v})$,

where $\vec{v} - T(\vec{v}) \in \ker T$ and $T(\vec{v}) \in \text{Im}(T)$. Note that $\text{Im}(T) \cap \ker(T) = \vec{0}$ since $T^2 = T$. Thus by Proposition 2.15 we see that

$$\mathbb{F}_q^n = U_1 \oplus \dots \oplus U_t = \text{Im}(T) \oplus \ker(T) = U_i \oplus \ker(T),$$

i.e. $\ker(T) = U_1 \oplus \dots \oplus U_{i-1} \oplus U_{i+1} \oplus \dots \oplus U_t$. Then for any $\vec{v} \in \mathbb{F}_q^n$ we have $\vec{v} = \vec{v}_1 + \dots + \vec{v}_t$, with $\vec{v}_j \in U_j$, and by (c) we can conclude that

$$T(\vec{v}) = T(\vec{v}_1 + \dots + \vec{v}_t) = T(\vec{v}_1) + \dots + T(\vec{v}_t) = T(\vec{v}_i) = \vec{v}_i = e_i(T_f)\vec{v}_i = e_i(T_f)(\vec{v}),$$

i.e. $T = e_i(T_f)$.

(e) For every $\vec{v} \in \mathbb{F}_q^n$, we have $\vec{v} = \vec{v}_1 + \dots + \vec{v}_t$ with $\vec{v}_i \in U_i$ for any $i = 1, \dots, t$. Thus by (c) and (d) we obtain that

$$\left(\sum_{i=1}^t e_i(T_f) \right) (\vec{v}) = \sum_{i=1}^t e_i(T_f)(\vec{v}_i) = \sum_{i=1}^t \vec{v}_i = \text{id}(\vec{v}).$$

(f) If $\vec{u}_i \in U_i$, then from (d) it follows that $\vec{u}_i = \vec{u}_i e_i(A) \in \langle e_i(A)_1, \dots, e_i(A)_n \rangle$, i.e. $U_i \subseteq \langle e_i(A)_1, \dots, e_i(A)_n \rangle$. Moreover, note that there exists a polynomial $s \in R$ such that $e_i(A) \cdot f_i^{\alpha_i}(A) = (e_i f_i^{\alpha_i})(A) = (sf)(A) = s(A)f(A) = 0$, that is, all the rows of $e_i(A)$ belong to U_i . Hence $\langle e_i(A)_1, \dots, e_i(A)_n \rangle \subseteq U_i$, i.e. $U_i = \langle e_i(A)_1, \dots, e_i(A)_n \rangle$. \square

3. FURTHER PROPERTIES OF SKEW GC CODES WITH $\delta_\beta^\theta = 0$

In this last section, we give some further results when the derivation δ_β^θ is zero, e.g., when either $\beta = 0$, or $\theta = \text{id}$.

3.1. The minimal polynomial of a semi-linear transformation. From Proposition 2.16 we know that $f \in N(R)$ if and only if $f(T_f) = 0$. In this subsection we show how to construct the minimal polynomial of any semi-linear transformation $T := \Theta \circ M$ defined over \mathbb{F}_q^n .

Lemma 3.1. *Let $T := \Theta \circ M$ be a θ -semi-linear transformation on \mathbb{F}_q^n . Then*

$$T \cdot \lambda = \theta(\lambda) \cdot T \quad \forall \lambda \in \mathbb{F}_q.$$

Proof. Take a vector $\vec{v} \in \mathbb{F}_q^n$ and an element $\lambda \in \mathbb{F}_q$. Then

$$(T \cdot \lambda)(\vec{v}) = T(\lambda \vec{v}) = (\lambda \vec{v})\Theta \circ M = ((\vec{v})\Theta \circ M)\theta(\lambda) = \theta(\lambda) (T(\vec{v})) = (\theta(\lambda)T)(\vec{v}),$$

that is, $T \cdot \lambda = \theta(\lambda) \cdot T$ for any $\lambda \in \mathbb{F}_q$. \square

Note that by Lemma 3.1 one can consider the surjective ring homomorphism

$$\sigma : \mathbb{F}_q[X; \theta] \rightarrow \mathbb{F}_q[T; \theta],$$

defined by $p \mapsto p(T)$, where $\mathbb{F}_q[Z; \theta] := \mathbb{F}_q[Z; \theta, 0]$.

First of all, let us show that for any semi-linear transformation $T = \Theta \circ M$, there exists always a unique monic minimal polynomial $m_T \in \mathbb{F}_q[X; \theta]$ such that $m_T(T) = O$, where $O : \mathbb{F}_q^n \rightarrow \mathbb{F}_q^n$ is the null-map.

Let k be the order of θ , that is, $\theta^k = \text{id}$. Then by [8, Lemma 4] we have

$$\begin{aligned} T^k &= (\Theta \circ M)^k \\ &= \Theta^k M_{\theta^{k-1}} M_{\theta^{k-2}} \dots M_\theta M \\ &= \text{id} \circ B = B, \end{aligned}$$

where $B := M_{\theta^{k-1}} M_{\theta^{k-2}} \dots M_{\theta} M$ is a matrix with coefficients in \mathbb{F}_q . Therefore, there exists a (minimal) polynomial $m_B = X^h + b_{h-1}X^{h-1} + \dots + b_1X + b_0 \in \mathbb{F}_q[X]$ such that

$$m_B(B) = O = (T^k)^h + b_{h-1}(T^k)^{h-1} + \dots + b_1(T^k) + b_0(id).$$

This gives a polynomial $m := m_B(X^k) \in \mathbb{F}_q[X; \theta]$ such that $m(T) = O$, showing the existence of a unique minimal monic polynomial $m_T \in \mathbb{F}_q[X; \theta]$ such that $m_T(T) = O$. In fact, we can prove the following

Proposition 3.2. *Let $T := \Theta \circ M$ be a θ -semi-linear transformation on \mathbb{F}_q^n such that M is an invertible $n \times n$ matrix. Then the unique minimal monic polynomial $m_T \in \mathbb{F}_q[X; \theta]$ such that $m_T(T) = O$ is given by $m_T = m_B(X^k) \in \mathbb{F}_q^\theta[X; \theta]$, where k is the order of θ , m_B is the minimal monic polynomial of the $n \times n$ matrix $B := M_{\theta^{k-1}} M_{\theta^{k-2}} \dots M_{\theta} M$ and \mathbb{F}_q^θ is the field fixed by θ .*

Proof. Let $m_T \in \mathbb{F}_q[X; \theta]$ be the unique minimal monic polynomial such that $m_T(T) = O$. Take any polynomial $a \in \mathbb{F}_q[X; \theta]$ and write $a \cdot m_T = m_T \cdot q + r$, where r is the remainder of the left division of $a \cdot m_T$ by m_T . Since σ is a ring homomorphism, we have

$$\begin{aligned} O &= a(T) \cdot m_T(T) = \sigma(a) \cdot \sigma(m_T) = \sigma(a \cdot m_T) = \sigma(m_T \cdot q + r) = \sigma(m_T \cdot q) + \sigma(r) = \\ &= \sigma(m_T) \cdot \sigma(q) + \sigma(r) = m_T(T) \cdot q(T) + r(T) = r(T). \end{aligned}$$

By the minimality of m_T , we deduce that $r = 0$. Then $a \cdot m_T = m_T \cdot q$ for some $q \in \mathbb{F}_q[X; \theta]$. This shows that $Rm_T = m_TR = (m_T)$, i.e. m_T is an invariant polynomial in $\mathbb{F}_q[X; \theta]$. So $m_T = X^t \cdot b = b \cdot X^t$ for an integer $t \in \mathbb{Z}_{\geq 0}$ and some $b \in \mathbb{F}_q^\theta[X^k; \theta]$. Since M is an invertible $n \times n$ matrix, we deduce that T is an invertible map. Hence $O = m_T(T) = T^t b(T)$ implies $b(T) = O$, i.e. $m_T = b$ with $\deg m_T = sk$ for some $s \in \mathbb{Z}_{\geq 1}$ by the minimality of m_T . Since $T^k = B$, we conclude that $O = m_T(T) = p(B)$ for a polynomial $p \in \mathbb{F}_q^\theta[X; \theta]$ with $s = \deg p \geq \deg m_B$. Thus we get $m_T(T) = m_B(X^k) \in \mathbb{F}_q^\theta[X; \theta]$. \square

This allows us to obtain the following

Theorem 3.3. *Let $T := \Theta \circ M$ be a θ -semi-linear transformation on \mathbb{F}_q^n such that M is an invertible $n \times n$ matrix. Then there exists a ring isomorphism*

$$\mathbb{F}_q[X; \theta] / (m_B(X^k)) \cong \mathbb{F}_q[T; \theta]$$

defined by $[p] \mapsto p(T)$, where $[p]$ is the class of a polynomial $p \in \mathbb{F}_q[X; \theta]$, k is the order of θ and $m_B \in \mathbb{F}_q^\theta[X; \theta]$ is the monic minimal polynomial of the $n \times n$ matrix $B := M_{\theta^{k-1}} M_{\theta^{k-2}} \dots M_{\theta} M$.

Proof. Consider the ring homomorphism $\sigma : \mathbb{F}_q[X; \theta] \rightarrow \mathbb{F}_q[T; \theta]$, defined by $p \mapsto p(T)$. By construction, σ is surjective. Moreover, by Proposition 3.2 note that $\ker(\sigma) = (m_T)$. Then there exists an isomorphism $\bar{\sigma}$ between $\mathbb{F}_q[X; \theta] / (m_T)$ and $\mathbb{F}_q[T; \theta]$, where $\bar{\sigma}$ is defined by $[p] \mapsto p(T)$ and $[p]$ is the class of a polynomial p . \square

Remark 3.4. *If $p = q$ in $\mathbb{F}_q[X; \theta]$, then $[p] = [q]$ in $\mathbb{F}_q[X; \theta] / (m_B(X^k))$. Thus $p(T) = q(T)$ via $\bar{\sigma}$. Moreover, when $\theta = id$, from Theorem 3.3 we deduce that there exists a ring isomorphism*

$$\mathbb{F}_q[X] / (m_M) \cong \mathbb{F}_q[M]$$

defined by $[p] \mapsto p(M)$, where $[p]$ is the class of a polynomial $p \in \mathbb{F}_q[X]$ and $m_M \in \mathbb{F}_q[X]$ is the monic minimal polynomial of the $n \times n$ matrix M .

3.2. BCH lower bounds for the minimum distance. In this subsection we show some results which give lower bounds for the distance of a skew GC-code.

Assume that

$$f = X^n - f_{n-1}X^{n-1} - \dots - f_1X - f_0,$$

where $f_{n-1}, \dots, f_1, f_0 \in \mathbb{F}_q$ and $f_0 \neq 0$.

Lemma 3.5. *In R/Rf we have*

$$\alpha \cdot X = 1 \quad \text{and} \quad X \cdot \beta = 1,$$

where

$$\alpha := f_0^{-1}X^{n-1} - f_0^{-1}f_{n-1}X^{n-2} - \dots - f_0^{-1}f_2X - f_0^{-1}f_1$$

and

$$\beta := \theta^{-1}(f_0^{-1})X^{n-1} - \theta^{-1}(f_0^{-1}f_{n-1})X^{n-2} - \dots - \theta^{-1}(f_0^{-1}f_1).$$

In particular, when $\theta = \text{id}$, we get $X \cdot \alpha = \alpha \cdot X = 1$.

Proof. It is sufficient to note that in R/Rf we have the following equivalences:

$$\begin{aligned} X^n - f_{n-1}X^{n-1} - \dots - f_1X - f_0 &= 0 \iff \\ \iff (X^{n-1} - f_{n-1}X^{n-2} - \dots - f_1) \cdot X &= f_0 \\ \iff (f_0^{-1}X^{n-1} - f_0^{-1}f_{n-1}X^{n-2} - \dots - f_0^{-1}f_2X - f_0^{-1}f_1) \cdot X &= 1 \end{aligned}$$

and

$$\begin{aligned} X^n - f_{n-1}X^{n-1} - \dots - f_1X - f_0 &= 0 \\ \iff f_0^{-1}X^n - f_0^{-1}f_{n-1}X^{n-1} - \dots - f_0^{-1}f_1X &= 1 \\ \iff X \cdot (\theta^{-1}(f_0^{-1})X^{n-1} - \theta^{-1}(f_0^{-1}f_{n-1})X^{n-2} - \dots - \theta^{-1}(f_0^{-1}f_1)) &= 1. \end{aligned}$$

□

Let $\vec{v} \in \mathbb{F}_q^n$. We will denote by $\text{wt}(v)$ the Hamming weight of \vec{v} , where $\pi_f(\vec{v}) = v \in R/Rf$.

Lemma 3.6. *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a skew GC code, and consider a polynomial $c \in \pi_f(\mathcal{C})$ with weight $\text{wt}(c) = w$. Then, there exists $h \in R$ such that*

$$h \cdot c = 1 + \sum_{i=1}^{w-1} c_i X^{a_i} \in \pi_f(\mathcal{C}),$$

where $c_i \in \mathbb{F}_q^*$ and $a_i \in \mathbb{N}$ with $a_i \leq n-1$ for $i = 1, \dots, w-1$. Furthermore,

$$\text{wt}(h \cdot c) = \text{wt}\left(1 + \sum_{i=1}^{w-1} c_i X^{a_i}\right) = w.$$

Proof. Since $\text{wt}(c) = w$, we can write $c = b_{i_0}X^{i_0} + b_{i_1}X^{i_1} + \dots + b_{i_{w-1}}X^{i_{w-1}}$, where $i_0 < \dots < i_{w-1}$ and $b_{i_j} \neq 0$ for $j = 0, \dots, w-1$. Hence

$$c = b_{i_0}X^{i_0}(1 + \theta^{-i_0}(b_{i_0}^{-1}b_{i_1})X^{i_1-i_0} + \dots + \theta^{-i_0}(b_{i_0}^{-1}b_{i_{w-1}})X^{i_{w-1}-i_0}).$$

Since \mathcal{C} is a skew GC code, we can conclude that

$$\alpha^{i_0}b_{i_0}^{-1}c = 1 + \theta^{-i_0}(b_{i_0}^{-1}b_{i_1})X^{i_1-i_0} + \dots + \theta^{-i_0}(b_{i_0}^{-1}b_{i_{w-1}})X^{i_{w-1}-i_0} \in \pi_f(\mathcal{C}).$$

The statement follows by putting $h = \alpha^{i_0}b_{i_0}^{-1}$, $c_j = \theta^{-i_0}(b_{i_0}^{-1}b_{i_j})$ and $a_j = i_j - i_0$ for $j = 0, \dots, w-1$. □

Definition 3.7. Let $\mathcal{C} \subset \mathbb{F}_q$ be a skew GC code. The distance $d_{\mathcal{C}}$ of \mathcal{C} is defined as

$$d_{\mathcal{C}} := \min\{d(\vec{x}, \vec{y}) : \vec{x}, \vec{y} \in \mathcal{C}, \vec{x} \neq \vec{y}\},$$

where d is the Hamming distance.

Remark 3.8. Consider an element β in $\overline{\mathbb{F}_q}$ such that $p(\beta^k) = 0$, for some $p \in R$ and $k \in \mathbb{Z}_{>0}$. Then, from [8] it follows that there exists $q \in R$ such that

$$\beta^m - 1 = q(\beta)p(\beta),$$

i.e. $\beta^m = 1$ for some $m \in \mathbb{N}^*$. Hence, $\text{ord}(\beta) < +\infty$, where $\text{ord}(\beta)$ denotes the order of β .

Inspired by [4], the following results provide lower bounds on the minimum Hamming distance for a skew GC code.

Theorem 3.9. Let $\mathcal{C} = (g)_{n,q}^{\theta,0}$ be a skew GC code. Suppose there exists $\beta \in \overline{\mathbb{F}_q}$, $l \in \mathbb{Z}_{\geq 0}$, $c \in \mathbb{Z}_{>0}$ such that $g(\beta^{l+ci}) = 0$ for $i = 0, \dots, \delta - 2$. If $N_i(\beta^c) \neq 1$ for every $i = 1, \dots, n - 1$, then $d_{\mathcal{C}} \geq \delta$.

Proof. Suppose there exists a polynomial $c \in \pi_f(\mathcal{C})$ with $\text{wt}(c) = w < \delta$. By Lemma 3.6, we can assume that c is the following type

$$c = 1 + \sum_{i=1}^{w-1} c_i X^{a_i}$$

where $c_i \in \mathbb{F}_q^*$ and $a_i \in \mathbb{Z}_{>0}$ with $a_i < n$ for $i = 1, \dots, w - 1$. Define

$$Y_i := N_{a_i}(\beta) \quad , \quad S_j := \sum_{i=1}^{w-1} c_i Y_i^j = c(\beta^j) - 1.$$

and

$$\begin{aligned} p &:= \prod_{i=1}^{w-1} (X - Y_i^c) \\ &= X^{w-1} + p_1 X^{w-2} + \dots + p_{w-2} X + p_{w-1} \in \mathbb{F}_q[X]. \end{aligned}$$

Since by hypothesis $Y_i^c = N_{a_i}(\beta^c) \neq 1$, we deduce that $p(1) \neq 0$.

By arguing as in [4], we have the following equalities:

$$\begin{aligned} 0 &= \sum_{i=1}^{w-1} c_i Y_i^l p(Y_i^c) \\ &= \sum_{i=1}^{w-1} c_i Y_i^l \left(Y_i^{c(w-1)} + p_1 Y_i^{c(w-2)} + \dots + p_{w-2} Y_i^c + p_{w-1} \right) \\ &= \sum_{i=1}^{w-1} c_i \left(Y_i^{l+c(w-1)} + p_1 Y_i^{l+c(w-2)} + \dots + p_{w-2} Y_i^{l+c} + p_{w-1} Y_i^l \right) \\ &= \sum_{i=1}^{w-1} c_i Y_i^{l+c(w-1)} + p_1 \left(\sum_{i=1}^{w-1} c_i Y_i^{l+c(w-2)} \right) + \dots + p_{w-2} \left(\sum_{i=1}^{w-1} c_i Y_i^{l+c} \right) + \\ &\quad + p_{w-1} \left(\sum_{i=1}^{w-1} c_i Y_i^l \right) = S_{l+c(w-1)} + p_1 S_{l+c(w-2)} + \dots + p_{w-2} S_{l+c} + p_{w-1} S_l \end{aligned}$$

i.e.

$$S_{l+c(w-1)} + p_1 S_{l+c(w-2)} + \dots + p_{w-2} S_{l+c} + p_{w-1} S_l = 0. \quad (*)$$

Since $c \in \pi_f(\mathcal{C})$, we have $c(\beta^{l+ci}) = 0$ for $i = 0, \dots, \delta - 2$. Then

$$S_{l+ci} = c(\beta^{l+ci}) - 1 = -1$$

for every $i = 0, \dots, \delta - 2$. So by $(*)$ we conclude

$$0 = S_{l+c(w-1)} + p_1 S_{l+c(w-2)} + \dots + p_{w-2} S_{l+c} + p_{w-1} S_l = -p(1),$$

i.e. $p(1) = 0$, a contradiction. Hence $d_{\mathcal{C}} \geq \delta$. \square

Remark 3.10. *The condition $\text{rk } V_n(N_0(\beta^c), N_1(\beta^c), \dots, N_{n-1}(\beta^c)) = n$ implies the hypothesis of the above result. Thus Theorem 3.9 generalizes Theorem 4 of [2] when the derivation is trivial.*

Example 3.11. *Assume that $\theta = \text{id}$. Then the assumptions $\text{ord}(\beta) \geq n$ and $\gcd(\text{ord}(\beta), c) = 1$ imply the hypothesis $\beta^{a_i c} \neq 1$ of Theorem 3.9 for every $i = 1, \dots, n-1$. Moreover, if only the hypothesis $\text{ord}(\beta) \geq n$ holds, then the distance of the code may be less than the expected lower bound. For instance, consider the vector space \mathbb{F}_7^6 with $\beta = 5$, $c = 4$ and $l = 1$. Then the GC code $\mathcal{C} = ((X-5)(X-3))_{6,7}^{\text{id},0}$ has distance $2 < 3$.*

The following result is a generalization of the above theorem and in some circumstances gives a better lower bound than that of Theorem 3.9.

Theorem 3.12. *Let $\mathcal{C} = (g)_{n,q}^{\theta,0}$ be a skew GC code. Suppose there exist $\beta \in \overline{\mathbb{F}_q}$, $l, c_1, c_2 \in \mathbb{Z}_{\geq 0}$ such that $(c_1, c_2) \neq (0, 0)$, $g(\beta^{l+c_1 i_1 + c_2 i_2}) = 0$ for $i_1 = 0, \dots, \delta - 2$ and $i_2 = 0, \dots, s$. If $N_i(\beta^{c_j}) \neq 1$ for every $i = 1, \dots, n-1$ and $j = 1, 2$, then we have $d_{\mathcal{C}} \geq \delta + s$.*

Proof. By Theorem 3.9 it follows that, $d_{\mathcal{C}} \geq \delta$. Suppose there exist an element $c \in \pi_f(\mathcal{C})$ with $\text{wt}(c) = w$ such that $\delta \leq w < \delta + s$. By Lemma 3.6, as in the Proof of Theorem 3.9 write

$$c = 1 + \sum_{i=1}^{w-1} c_i X^{a_i}$$

where $c_i \in \mathbb{F}_q^*$ and $a_i \in \mathbb{Z}_{>0}$ with $a_i < n$ for $i = 1, \dots, w-1$.

Similarly to Theorem 3.9, define again

$$Y_i := N_{a_i}(\beta) \quad , \quad S_j := \sum_{i=1}^{w-1} c_i Y_i^j = c(\beta^j) - 1$$

and

$$\begin{aligned} p &:= \prod_{i_1=1}^{\delta-2} (X - Y_{i_1}^{c_1}) \\ &= X^{\delta-2} + p_1 X^{\delta-3} + \dots + p_{\delta-3} X + p_{\delta-2} \in \mathbb{F}_q[X], \\ q &:= \prod_{i_2=\delta-1}^{w-1} (X - Y_{i_2}^{c_2}) \\ &= X^{w-\delta+1} + q_1 X^{w-\delta} + \dots + q_{w-\delta} X + q_{w-\delta+1} \in \mathbb{F}_q[X], \\ r &:= pq \end{aligned}$$

Since $Y_{i_j}^{c_j} = N_{a_{i_j}}(\beta^{c_j}) \neq 1$ for $j = 1, 2$, we see that $r(1) \neq 0$.

On the other hand, we have the following equalities:

$$\begin{aligned}
0 &= \sum_{i=1}^{w-1} c_i Y_i^l p(Y_i^{c_1}) q(Y_i^{c_2}) \\
&= \sum_{i=1}^{w-1} c_i Y_i^l (Y_i^{c_1(\delta-2)} + p_1 Y_i^{c_1(\delta-3)} + \dots + p_{\delta-2} Y_i^{c_1(w-\delta+1)} + q_1 Y_i^{c_2(w-\delta)} + \\
&\quad + \dots + q_{w-\delta+1}) \\
&= \sum_{i=1}^{w-1} c_i [(Y_i^{l+c_1(\delta-2)} + p_1 Y_i^{l+c_1(\delta-3)} + \dots + p_{\delta-2} Y_i^l) (Y_i^{c_2(w-\delta+1)} + q_1 Y_i^{c_2(w-\delta)} + \\
&\quad + \dots + q_{w-\delta+1})] \\
&= \sum_{i=1}^{w-1} c_i [(Y_i^{l+c_1(\delta-2)+c_2(w-\delta+1)} + p_1 Y_i^{l+c_1(\delta-3)+c_2(w-\delta+1)} + \dots + p_{\delta-2} Y_i^{l+c_2(w-\delta+1)}) + \\
&\quad + q_1 (Y_i^{l+c_1(\delta-2)+c_2(w-\delta)} + p_1 Y_i^{l+c_1(\delta-3)+c_2(w-\delta)} + \dots + p_{\delta-2} Y_i^{l+c_2(w-\delta)}) + \dots + \\
&\quad + q_{w-\delta+1} (Y_i^{l+c_1(\delta-2)} + p_1 Y_i^{l+c_1(\delta-3)} + \dots + p_{\delta-2} Y_i^l)] \\
&= (S_{l+c_1(\delta-2)+c_2(w-\delta+1)} + p_1 S_{l+c_1(\delta-3)+c_2(w-\delta+1)} + \dots + p_{\delta-2} S_{l+c_2(w-\delta+1)}) + \dots + \\
&\quad + q_1 (S_{l+c_1(\delta-2)+c_2(w-\delta)} + p_1 S_{l+c_1(\delta-3)+c_2(w-\delta)} + \dots + p_{\delta-2} S_{l+c_2(w-\delta)}) + \dots + \\
&\quad + q_{w-\delta+1} (S_{l+c_1(\delta-2)} + p_1 S_{l+c_1(\delta-3)} + \dots + p_{\delta-2} S_l).
\end{aligned}$$

Since $c \in \pi_f(\mathcal{C})$ we know that $c(\beta^{l+c_1 i_1+c_2 i_2}) = 0$. Hence

$$S_{l+c_1 i_1+c_2 i_2} = c(\beta^{l+c_1 i_1+c_2 i_2}) - 1 = -1,$$

for $i_1 = 0, \dots, \delta-2$, $i_2 = 0, \dots, s$ and $\delta \leq w < \delta + s$. Therefore from the above equation and the inequalities, we can conclude

$$0 = (1 + q_1 + \dots + q_{w-\delta} + q_{w-\delta+1})(-1 - p_1 - \dots - p_{\delta-3} - p_{\delta-2}) = -r(1),$$

i.e. $r(1) = 0$, but this give a contradiction. Hence $d_{\mathcal{C}} \geq \delta + s$. \square

Remark 3.13. The condition $\text{rk } V_n(N_0(\beta^{c_j}), N_1(\beta^{c_j}), \dots, N_{n-1}(\beta^{c_j})) = n$ for $j = 1, 2$ implies the hypothesis of Theorem 3.12.

Remark 3.14. Assume that $\theta = \text{id}$. Then the assumptions $\text{ord}(\beta) \geq n$ and $\text{gcd}(\text{ord}(\beta), c_j) = 1$ for $j = 1, 2$ imply the hypothesis $\beta^{a_i c_j} \neq 1$ of Theorem 3.12 for every $i = 1, \dots, n-1$ and $j = 1, 2$. Furthermore, we get the following properties:

- (a) Let $X^m - 1 = qf$ be as in [8, Lemma 26]. If $\text{gcd}(m, \text{Char}(\mathbb{F}_q)) = 1$, then there exist a primitive root $\beta \in \mathbb{F}_q^*$ of $X^m - 1$ such that $\text{ord}(\beta) = m \geq n$. Moreover, if $g(\alpha) = 0$ then $\alpha = \beta^h$ for some $h \in \mathbb{Z}_{\geq 0}$.
- (b) Let $f = X^n - 1$. Suppose there exists a primitive root β of f . Then all roots α of g are of type $\alpha = \beta^h$ for some $h \in \mathbb{Z}_{\geq 0}$. Moreover, the hypothesis of Theorem 3.9 reduce to that of Theorem 1 in [4] when $\theta = \text{id}$.

Let us give now a natural extension of Theorem 3.12, which can be proved by an inductive argument.

Theorem 3.15. Let $\mathcal{C} = (g)_{n,q}^{\theta,0}$ be a skew GC code. Suppose there exist $\beta \in \overline{\mathbb{F}_q}$ and $l, c_1, \dots, c_r \in \mathbb{Z}_{\geq 0}$ such that $(c_1, \dots, c_r) \neq (0, \dots, 0)$ and $g(\beta^{l+\sum_{k=1}^r i_k c_k}) = 0$ for $i_1 = 0, \dots, \delta - 2$, $i_k = 0, \dots, s_k$ and $k = 2, \dots, r$. If $N_i(\beta^{c_j}) \neq 1$ for every $i = 1, \dots, n - 1$ and $j = 1, \dots, r$, then $d_{\mathcal{C}} \geq \delta + \sum_{k=2}^r s_k$.

Remark 3.16. If $\beta \in \mathbb{F}_q$, then $\text{ord}(\beta) \leq q - 1$ and in Theorem 3.15 the hypothesis imply that $q \geq n + 1$.

Corollary 3.17. Let $\mathcal{C} = (g)_{n,q}^{\theta,0}$ with $q \geq n + 1$. If $\beta \in \mathbb{F}_q$, $l, c_1, \dots, c_r \in \mathbb{Z}_{\geq 0}$ such that $(c_1, \dots, c_r) \neq (0, \dots, 0)$,

$$g = \text{lcm} \{ X - \beta^{l+\sum_{k=1}^r i_k c_k} : i_1 = 0, \dots, \delta, i_k = 0, \dots, s_k, k = 2, \dots, r, \delta + \sum_{k=2}^r s_k = n - k - 1 \},$$

and $N_i(\beta^{c_j}) \neq 1$ for every $i = 1, \dots, n - 1$ and $j = 1, \dots, r$, then \mathcal{C} is a Maximum Distance Separable (MDS) code.

Proof. Since $\deg(g) \leq n - k$, by the Singleton bound we know that

$$d_{\mathcal{C}} \leq n - \dim(\mathcal{C}) + 1 = n - (n - \deg(g)) + 1 \leq n - k + 1.$$

On the other hand, from Theorem 3.15 it follows that $d_{\mathcal{C}} \geq n - k + 1$, i.e. $d_{\mathcal{C}} = n - k + 1$. \square

4. MAGMA PROGRAMS AND SOME EXAMPLES

The following MAGMA [1] program can be used to produce MDS codes with $q \geq n + 1$ when $\theta = id$:

```
MDS:=function(q,n);
F<w>:=GF(q); R<x>:=PolynomialRing(F); C:={};
for i in [1..q-2] do
  if GCD(i,q-1) eq 1 then
    C:=C join {i};
  end if;
end for;
CC:=[c : c in C]; B:={};
for c in CC do
  for l in [0..q-2] do
    for k in [1..n-1] do
      A:=[ (w^l)*(w^c)^i : i in [0..n-k-1] ]; B:=B join {A};
    end for;
  end for;
end for;
BB:=[ b : b in B ]; D:=[ [x-i : i in BB[j] ] : j in [1..#BB] ];
G:={ &*D[i] : i in [1..#D] }; GG:=[g : g in G]; W1:={}; W2:={};
for s in [1..#GG] do
  h:=n-Degree(GG[s]); M:=Matrix(F,h,n,[ Coefficient((GG[s])*x^i,j):
  j in [0..n-1] ] : i in [0..h-1] ); L:=LinearCode(M);
  d:=MinimumWeight(L); v:=Matrix(Integers(),1,4,[n,h,d,q]); g:=GG[s];
  print "q =", q; print "Code of type", v; print "Generator polynomial", g;
  for i in E do
    a,b:=Quotrem(x^n-i,g);
    if b eq R!0 then
```



```

    print "Constacyclic code with f =", x^n-i;
  end if;
end for;
W1:=W1 join {v}; W2:=W2 join {g};
end for;
return W1;
end function;

```

The following table is made in the case $\theta = id$ by using the command $\text{MDS}(q,n)$;
of the above Magma Program for $2 \leq n \leq q-1 \leq 6$:

q	$n = \deg f$	k	d	g such that $g f$	a such that $f = X^n - a$
3	2	1	2	$x+2$	1
4	3	2	2	$x+w^2, x+w, x+1$	1
	1	3	3	$x^2+x+1, x^2+w^2x+w, x^2+wx+w^2$	1
5	2	1	2	$x+1, x+w, x+w^2$	$1, w^2, w$
	4	3	2	$x+4$	1
6	3	2	3	x^2+3x+1	$\#$
	1	4	4	x^3+2x^2+3x+4	$\#$
7	2	2	2	$x+4$	1
	1	3	3	x^2+3x+1	$\#$
8	2	1	2	$x+4$	1
	6	5	2	$x+6$	1
9	4	4	3	x^2+5x+1	$\#$
	3	3	4	x^3+4x^2+3x+6	$\#$
10	2	5	5	$x^4+3x^3+6x^2+3x+1$	$\#$
	1	6	6	$x^5+2x^4+3x^3+4x^2+5x+6$	$\#$
11	4	4	2	$x+6$	1
	3	3	3	x^2+5x+1	$\#$
12	2	4	4	x^3+4x^2+3x+6	$\#$
	1	5	5	$x^4+3x^3+6x^2+3x+1$	$\#$
13	4	3	2	$x+6$	1
	3	2	3	x^2+5x+1	$\#$
14	2	1	4	x^3+4x^2+3x+6	$\#$
	1	2	2	$x+6$	1
15	3	1	3	x^2+5x+1	$\#$
	2	1	2	$x+6$	1

Table 1: Example of MDS codes in \mathbb{F}_q^n for $q \leq 7$ with $n \leq q-1 \leq 6$

The following two MAGMA [1] programs can be used to construct all the $(f, \Theta, 0)$ -skew GC codes over \mathbb{F}_q^n for any polynomial $f \in \mathbb{F}_q[X; \theta]$ given in its vectorial form in the non-commutative ($\theta \neq id$) and commutative cases ($\theta = id$) respectively:

```

a:= ... ;
F<w>:=GF(a);

// PROGRAM 1 (non-commutative case)

R<X>:=TwistedPolynomials(F;q:= ...);

SkewGCC:=function(v);
f:=R!v; n:=Degree(f); V:=VectorSpace(F,n); W1:=[]; W2:=[]; dd:=[];
E:=[x : x in F | x ne 0]; S:=CartesianProduct(E,CartesianPower(F,n-1));
for ss in S do
  ll:=[ss[1]] cat [p : p in ss[2]]; q,r:=Quotrem(f,R!ll);
  if r eq R![0] then
    dd := dd cat [R!ll];
  end if;
end for;
return dd;
end function;

```

```

    end if;
end for;
for i in [1.. #dd] do
  if Degree(dd[i]) ge 1 then
    k:=Degree(f)-Degree(dd[i]);
    G:=Matrix(F,k,n,[V!(HorizontalJoin(Matrix(1, j+Degree(dd[i])+1,
    Eltseq((R![0,1])^j*dd[i])), ZeroMatrix(F, 1, n-j-Degree(dd[i])-1)))):
    j in {0..k-1}]); L:=LinearCode(G); dd[i]; print " "; G; print " ";
    print "Code of type: ", n, k, MinimumWeight(L);
    print "-----"; W1:= W1 cat [k]; W2:= W2 cat [MinimumWeight(L)];
  end if;
end for;
print "Spectrum of the distances for", f;
print "n=", n; print "k="; W1; print "d=";
return W2;
end function;

// PROGRAM 2 (commutative case)

R<x> := PolynomialRing(F);

GCC:=function(v);
f:=R!v; n:=Degree(f); W1:=[]; W2:=[];
for i in [1..#Factorisation(f)] do
  if Factorisation(f)[i][2] eq 1 then
    a:=R!Factorisation(f)[i][1]; k:=Degree(f)-Degree(R!a);
    G:=Matrix(F,k,n,[Coefficient((R!a)*x^i,j): j in {0..n-1}]
    : i in {0..k-1}]); L:=LinearCode(G); a; print " "; G; print " ";
    print "Code of type: ", n, k, MinimumWeight(L);
    print "-----"; W1:= W1 cat [k]; W2:= W2 cat [MinimumWeight(L)];
  end if;
  if Factorisation(f)[i][2] ne 1 then
    for j in [1.. Factorisation(f)[i][2]] do
      a:=(R!Factorisation(f)[i][1])^j; k:=Degree(f)-Degree(R!a);
      G:=Matrix(F,k,n,[Coefficient((R!a)*x^i,j): j in {0..n-1}]
      : i in {0..k-1}]); L:=LinearCode(G); a; print " "; G; print " ";
      print "Code of type: ", n, k, MinimumWeight(L);
      print "-----"; W1:= W1 cat [k]; W2:= W2 cat [MinimumWeight(L)];
    end for;
  end if;
end for;
print "Spectrum of the distances for", f;
print "n=", n; print "k="; W1; print "d=";
return W2;
end function;

```

Example 4.1. Consider $f = X^4 + X^3 + wX^2 + 1 \in \mathbb{F}_8[X, \theta]$. If $\theta(z) = z^2$ for any $z \in \mathbb{F}_8$, then by PROGRAM 1 (with $v = [1, 0, w, 1, 1]$, $a = 8$ and $q := 2$) we obtain 28 MDS skew GC codes with parameters $[4, 1, 4]_8$, $[4, 2, 3]_8$ and $[4, 3, 2]_8$, while if

$\theta = \text{id}$, then by PROGRAM 2 (with $v = [1, 0, w, 1, 1]$, $a = 8$) we get only 2 MDS GC codes with parameters $[4, 1, 4]_8$ and $[4, 3, 2]_8$. Moreover, the MDS skew GC code of type $[4, 2, 3]_8$ is given, for instance, by the right divisor $X^2 + wX + w$ of f .

Example 4.2. Consider the finite field $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, θ the Frobenius automorphism and $\beta \in \mathbb{F}_4$. Let $f = X^8 + X^6 + X^2 + 1 \in N(R)$ with $R = \mathbb{F}_4[X, \theta, \delta_\beta]$ and note that $f = f_1^{\alpha_1} \cdot f_2^{\alpha_2}$ is a factorization of f as in (#), where $(f_1, \alpha_1) = (X^2 + 1, 2)$ and $(f_2, \alpha_2) = (X^4 + X^2 + 1, 1)$. Set $U_i := \text{Ker} f_i^{\alpha_i}(T_f)$ for $i = 1, 2$, where T_f is given by the following rule:

$$T_f(v_1, \dots, v_8) := (v_1^2, \dots, v_8^2) \begin{pmatrix} 0 & 1 & & & & & & \\ 0 & & 1 & & & & & \\ 0 & & & 1 & & & & \\ 0 & & & & 1 & & & \\ 0 & & & & & 1 & & \\ 0 & & & & & & 1 & \\ 0 & & & & & & & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} + \beta(v_1^2 - v_1, \dots, v_8^2 - v_8),$$

$$\text{i.e. } T_f(v_1, \dots, v_8) := (v_8^2, v_1^2, v_2^2 + v_8^2, v_3^2, v_4^2, v_5^2, v_6^2 + v_8^2, v_7^2) + \beta(v_1^2 - v_1, \dots, v_8^2 - v_8).$$

By the MAGMA program

```
F<w>:=GF(4); P<[x]>:=PolynomialRing(F,8); A:=KSpace(F,8); B:=[a : a in A];
for b in F do
T:= map < A -> A | v :-> [v[8]^2+b*(v[1]^2+v[1]), v[1]^2+b*(v[2]^2+v[2]),
v[8]^2+v[2]^2+b*(v[3]^2+v[3]), v[3]^2+b*(v[4]^2+v[4]),
v[4]^2+b*(v[5]^2+v[5]), v[5]^2+b*(v[6]^2+v[6]),
v[6]^2+v[8]^2+b*(v[7]^2+v[7]), v[7]^2+b*(v[8]^2+v[8])] >;
U1:={}; U2:={}; g:=T^4; h:=T^2; f1:= map < A -> A | x :-> g(x)+x >;
f2:= map < A -> A | x :-> g(x)+h(x)+x >; o:=A![0,0,0,0,0,0,0,0];
for a in B do
if f1(a) eq o then
U1:=U1 join {a};
end if;
if f2(a) eq o then
U2:=U2 join {a};
end if;
end for;
UU1:=[u : u in U1]; UU2:=[u : u in U2]; V1:={}; V2:={};
for i in [4..#UU1] do
for j in [4..#UU2] do
G1:= sub< A | UU1[1], UU1[2], UU1[i-1], UU1[i] >;
G2:= sub< A | UU2[1], UU2[2], UU2[j-1], UU2[j] >;
if Dimension(G1) eq 4 then
V1:= V1 join {Basis(G1)};
end if;
if Dimension(G2) eq 4 then
V2:= V2 join {Basis(G2)};
end if;
```

```

end for;
end for;
VV1:=[v : v in V1]; VV2:=[w : w in V2]; b; VV1[1]; VV2[1]; print "---";
end for;

```

we obtain the following table:

β	Generator matrix of U_1	Generator matrix of U_2
1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$
$0, w, w^2$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

Table 2: Example of skew GC codes in \mathbb{F}_4^8 with a non-trivial derivation

CONCLUSION

In this paper, we consider codes invariant by a pseudo-linear transformation of \mathbb{F}_q^n for $n \geq 2$, called skew generalized cyclic (GC) codes, where \mathbb{F}_q is a finite field with q elements. We study some of their main algebraic and geometric properties and when the derivation is trivial, we find the minimal polynomial of a pseudo-linear transformation and we give some lower bounds for the minimum Hamming distance of a skew GC code. Finally, examples and Magma programs are given as applications of some theoretical results.

REFERENCES

- [1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
- [2] D. Boucher and F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes Cryptogr. **70** (2014), no. 3, 405–431.
- [3] M’Hammed Boulagouaz, A. Leroy, (σ, δ) -codes, Adv. Math. Commun. **7** (2013), no. 4, 463–474.
- [4] C.R. Hartmann, K.K. Tzeng, *Generalizations of the BCH bound*, Information and Control **20** (1972), 489–498.
- [5] I.N. Herstein, *Topics in algebra*, 2nd Edition, Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975.
- [6] N. Jacobson, *The Theory of Rings*, American Mathematical Society Mathematical Surveys, vol. II. American Mathematical Society, New York, 1943.
- [7] D. Radkova, A.J. Van Zanten, *Constacyclic codes as invariant subspaces*, Linear Algebra Appl. **430** (2009), no. 2-3, 855–864.
- [8] L.F. Tapia Cuitiño, A.L. Tironi, *Dual codes of product semi-linear codes*, Linear Algebra Appl. **457** (2014), 114–153.

DEPARTAMENTO DE MATEMÁTICA, UNIVERSIDAD DE CONCEPCIÓN, CASILLA 160-C, CONCEPCIÓN, CHILE

E-mail address: ltapiac@udec.cl, atironi@udec.cl